Michigan Law Review

Volume 69 | Issue 7

1971

Miller: The Assault on Privacy

Michael S. Josephson
Wayne State University

RECENT BOOKS

Book Reviews

THE ASSAULT ON PRIVACY. *By Arthur R. Miller.* Ann Arbor, Mich.: The University of Michigan Press. 1971. Pp. 325. $7.95.

> In spite of the successful adjustment man has made to the machine in many contexts, it would be foolish not to recognize . . . [the effect] that certain applications of the computer may have on that elusive value we call "personal privacy." [p. 3.]
>
> This book . . . will not simply catalog the great strides being taken in the computer world or goggle over the predictions and projections of the scientific community's enthusiasts. Rather, its aim is to explore some of the ways in which information technology is altering basic patterns in our daily life and to evaluate the responses being made by the law, government, industry, and other institutions . . . . [p. 2.]

In these words Arthur R. Miller defines the task of *The Assault on Privacy*, a task the book carries out with a systematic, machine-like efficiency. While *The Assault on Privacy* is an unmistakable call to arms against a descending "dossier dictatorship," it avoids the strident generalizations and glib platitudes that often envelop works on the emotion-laden subject of privacy. Even as he trots out the familiar hypothetical parade of horribles,[1] Professor Miller demonstrates an admirable restraint and sense of perspective. Combining these features with the inexhaustible research of a true scholastic virtuoso, Professor Miller's book demands recognition as a genuinely outstanding contribution to the field of privacy protection.[2]

One of the most impressive aspects of the small volume is the extensive documentation that makes it an invaluable reference work. In order to give his assertions the tone of conclusive authority, Professor Miller has combed thousands of pages of congressional hearings, hundreds of periodicals and books by computerists, social scientists, and legal analysts, and the complete works of Shakespeare —all presumably without the aid of a computer.[3] While his insis-

1. No current work on privacy is complete without some catalog of the awful potential of modern surveillance technology. Professor Miller, for example, points out that it is possible to monitor a human being with sensors that can reveal his activities and emotions and that computer technology is such that information contained in a twenty-page dossier on every American could be stored for almost instant retrieval on one computer tape (pp. 12, 45-46).

2. In the opinion of the reviewer this is one of three important books in the privacy field. THE EAVESDROPPERS, by S. Dash, R. Schwartz & R. Knowlton (1959), sounded the first warning bell against the growing capabilities of electronic surveillance and was a major impetus to the first United States Supreme Court rejection of electronically seized evidence (Silverman v. United States, 365 U.S. 505 (1961)). The other major work is Alan Westin's complete treatise, PRIVACY AND FREEDOM (1967).

3. It is as if Professor Miller commanded a small army of researchers, but of course that would be impossible in today's tight budget situation.

tence on commencing each subsection of the book with a quotation, often of esoteric origin, sometimes seems a little pushy,[4] one is inclined to forgive him for this small vanity in view of the end product. From his description of computer technology and terminology to his review and analysis of the relevant law, Professor Miller convinces his reader that he knows what he is talking about.

In substance, the book argues that privacy is threatened by the growing use of computer technology and that safeguards are required if we are to limit the detrimental aspect of these omnipotent, omniscient tools.

> [T]he computer, with its insatiable appetite for information, its image of infallibility, and its inability to forget anything that has been stored in it, may become the heart of a surveillance system that will turn society into a transparent world in which our homes, our finances, and our associations will be bared to a wide range of casual observers, including the morbidly curious and the maliciously or commercially intrusive. [p. 3.]

One problem in protecting privacy from the probing button pushers of computer-based services is the apparent willingness of millions of citizens to trade personal information for the advantage of the issuance of credit, welfare payments, insurance, and the like. These institutional benefits are conferred only after machines have digested and analyzed large amounts of private data that must be supplied by the applicant, and getting the consent of the applicant to supply such data has presented no serious problem. Assuming, as Professor Miller does, the desirability and continued vitality of data-based services, the question becomes one of regulation rather than elimination. To use Miller's dimpled turn of a phrase, the question is, How to live with the computer?

I. Controlling the Use of Private Information

The thrust of Miller's proposals in this area focuses upon limiting the *use* of private data as opposed to its *acquisition*.[5] His use-oriented regulations revolve around the premise that personal information surrendered for a particular purpose and to a limited audience (*e.g.*, credit data given to a bank for purposes of a loan) should not be used for any other purpose or seen by any other audience (*e.g.*, the credit data should not be made available to po-

4 For esoteric sources, some all-time favorites can be found in The Assault on Privacy. Among the special gems are a limerick from the Hamilton College Alumni Review (p. 105); a quote from Viscount Buckmaster's Introduction to A. P. Herbert's Uncommon Law (p. 169); and a relevant word from Pope Pius XII in a speech delivered to the Congress of the International Association of Applied Psychology (p. 216).

5. For a laboring of this distinction, see Josephson, *Book Review*, 15 U.C.L.A. L. Rev. 1586, 1590-93 (1968).

tential employers). While this position is rooted in the traditional definition of privacy—the ability of a person to control the dissemination of information about himself—it is one that has not fared well in court. Therefore, the legal problems involved in such proposals do merit some attention.

Of particular relevance is the United States Supreme Court's handling of the unauthorized use of private information by an informant posing as a friend, co-conspirator, or confidant. Whether the informant utilizes a tape recorder, as in *Lopez v. United States*[6] and *Osborn v. United States*,[7] or merely serves as a human conduit to the police, as in *Hoffa v. United States*,[8] the Court has consistently held that once information is freely given, the giver loses his right to control its further use. The rationale of this result is that by choosing to reveal private information one assumes the risk that a confidant will betray him, and he will not be heard to protest the consequences of his misplaced confidence. Implicit in this holding is the theory that when information is released to another it is done wholly and unconditionally, regardless of the intentions of the speaker. Like the squeezing of toothpaste out of the tube, the revelation of private information is irrevocable.

It can be argued that the later case of *Katz v. United States*,[9] which defined constitutionally protected privacy in terms of one's "reasonable expectations," ought to modify these holdings and at least require an ad hoc determination of whether the speaker could have "reasonably expected" a particular confidant to transmit the information to the police. It is one thing to say that a night club proprietor could reasonably expect an IRS agent to reject a bribe and report the incident to his superiors,[10] and quite another to apply the same theory to a long-time friend and business associate.[11] Thus, *Katz* could be read to suggest that a person assumes the risk of betrayal only when he has no reasonable expectation of privacy, that careful selection of one's confidants is all that is required to invoke the protections of the fourth amendment. This is not, however, the present interpretation of the *Katz* case, and the reluctance of the courts to extend the scope of privacy and limit the use of conversations in the informant area ought to be considered in the context of restricting the use of voluntarily revealed personal data in the computer privacy setting.

Why should a man assume the risk that one who poses as his

6. 373 U.S. 427 (1963).
7. 385 U.S. 323 (1966).
8. 385 U.S. 293 (1966).
9. 389 U.S. 347 (1967).
10. Lopez v. United States, 373 U.S. 427 (1963).
11. Hoffa v. United States, 385 U.S. 293 (1966).

friend will abuse his trust and misuse information given him and yet not assume the same risk when dealing with an impersonal service organization? In terms of both the known risks and one's reasonable expectations, the arguments for a loss of control over personal information are stronger in the data-gathering context than in the court-considered informant situation. One who fills out a form or application as a condition precedent to a benefit he seeks *knows* that the information supplied may be read, checked, and examined by a number of strangers from clerks to investigators and programmers. By the test of *Lopez* and *Katz* the applicant has no reasonable expectation that these persons will act in good faith or with the utmost discretion, and he could be deemed to assume the risk that either the institution or its functionaries will use the information for other purposes. Furthermore, when the government attempts to limit the way in which certain information can be disseminated, there are significant free speech considerations to be met. If a credit company employee is, in essence, sworn to secrecy, may he be enjoined from testifying in court as well as gossiping to a friend? While such a problem is not insuperable, it is suggestive of the difficulties implicit in legislative attempts to limit the use of information.

The cases refusing to invoke the right of privacy in a constitutional sense are not applicable to legislative action that seeks to grant greater individual protections than the minimum standards set forth by the Supreme Court. This point is particularly evident as one shifts the focus from a criminal investigation context (in which the public interest in obtaining and using private information is somewhat compelling) to the powers of civil service-oriented institutions.

In addition, the rationale of the *Lopez* and *Katz* decisions is subject to direct frontal attack. The concept of viewing privacy in terms of one's reasonable expectations is laden with the seeds of self-destruction. If the question of privacy entails only the protection of one's actual expectations, without regard to justifiable claims for greater protection, the right of privacy will shrink in direct proportion to the expansion of surveillance practices. By disclaimer or by formal notice, the private credit company or the governmental agency could enlarge its right to use information merely by announcing its intention to do so. The readiness of persons to sign contracts with clauses that authorize extensive investigation and waive the signer's right to assert legislatively granted privileges demonstrates the ease with which individuals can be induced to barter their privacy protections for a present benefit. Thus, the implication of the reasonable expectation doctrine into the computer privacy area could sanction any use the information-gathering organization chose to make of personal data.

Finally, precedent for the control of private information can be found in the concept of legally protected privileges. Such privileges traditionally allow a client, a patient, or a penitent to prevent his attorney, doctor, or minister from revealing information transmitted in confidence in the course of their special relationship. It is not inconceivable that a similar privilege could be granted to the communication between a beneficiary (*e.g.*, credit or welfare applicant) and his intended benefactor.

II. Changing Concepts of Privacy

The direct dangers to privacy posed by insensitive computer operators may be minimized by careful regulation of the use of collected personal data. However, this approach assumes that the broad availability and distribution of the type of personal information involved is socially deleterious, an assumption subject to challenge. Professor Miller points out that

> the public may lose its sense of the private if large-scale transfers and dissemination of personal information become common. . . . People accustomed to the revelation of sensitive personal data eventually may define most information as public and place it beyond the law's protection. [p. 181.]

This observation reveals the fact that privacy is a changing concept that reflects social expectations. What is private at one time in history may be the subject of ostentatious exposure at another.[12] These changes result from an evolutionary modification of basic attitudes that are neither right nor wrong; they are merely different. Consequently, the fact that the public sense of privacy is being changed by the impact of computer technology may be part of a natural and healthy adaptation to an electronic era. In fact, this adaptation phenomenon may contain the solution to some of the negative implications of data surveillance. As the public becomes accustomed to the exposure of "personal" information, it is likely that the morbid curiosity of the gossip mongers will become sated[13] and the anxiety accompanying revelation will gradually disappear. In a world in

12. A short look at contemporary history illustrates the point. At the turn of the century the entire female body was a "no-peeking" preserve. The pulchritude of the ankle, calf, and thigh was carefully hidden as part of the private domain reserved for the good lady's husband. The "Peeping Tom" who stole a glimpse of a woman in a state of semi-undress truly violated that woman's privacy. Today, semi-nudity is a mode of dress which reflects a generation gap in privacy concepts. The point is that nothing is inherently private, that privacy reflects the mores of changing times.

13. The recent experience in Denmark with the Copenhagen sex shows wherein performers engaged in all forms of sexual activity on stage demonstrates how quickly the "excitingly different" can become gross exhibitionism. The triumph of the "Peeping" or "Listening" Tom is to see or hear something he is not supposed to witness. Take away the prohibition and you remove the incentive.

which everyone has access to the petty details of the lives of his neighbors, human foibles and misadventures become small in their proper perspective. In this light it may not be clear that the government ought to interfere by artificially reinforcing particular disposable notions of privacy.[14]

Much of the demand for privacy is a conditioned response. It can be posited that the sense of privacy is basically a product of the desire to defend oneself from public attitudes that do not coincide with certain personal behavior, that one seeks to keep private only that information that can harm him if disclosed. Privacy allows a person to project an image that is not a true reflection of his thoughts and conduct. The selection of the desired image and, consequently, the information to be kept from the public eye are usually a direct result of contemporary social norms. Thus, the kinds of things regarded as private vary according to acceptable social standards. Sexual behavior, for example, is not universally viewed as an activity that is to be blanketed by concepts of privacy. Even within the "civilized" nations there is a broad disparity in the type of information that is viewed as private and that which is viewed as not. A young unmarried woman in Sweden does not suffer a pang of discomfort if her employer learns she is living with her boy friend, while her Italian counterpart might feel that her private world has been invaded by such a disclosure. The difference is not related to the inherent moral quality of the conduct but to the capacity of the revealed fact to cause damage.

The assumption that the data accumulation of the computer violates privacy may also be attacked on the ground that the kind of information collected is not really private in nature. While the typical pro-privacy ploy is to hypothesize a surveillance device in the bedroom, recording and reporting the most intimate activities, the reality is that the type of information generally involved is already semi-public. For example, what a person earns is known by literally dozens of comparative strangers, his employer, the payroll clerk, those who cash the check, his family, his creditors, tax men, and often co-workers. Similarly, an individual's employment experience or contact with the law is a matter of record. The intrusiveness of the complete dossier comes from its ability to piece together hundreds of known facts into a total revealing picture. It is a case in which the sum is greater than its component parts.[15] The right to privacy

14. In purporting to defend a person's prerogative to preserve the privacy of primarily nonpernicious information, perhaps Professor Miller's proposals only protect his personal sense of propriety premised upon outmoded and artificial precepts.

15. For example, Professor Miller points out that the average person leaves clear tracks of his life through such things as airline and hotel reservations, credit card slips, canceled checks, and telephone records. However, only the detective who has access to all the information can accurately determine the subject's spending habits, his associations and, at the same time, reconstruct his activities.

in this context is nothing more than the right to prevent available, freely given, nonintimate information from being collected and stored in one place. In essence, as society's detective capacities become efficient enough to evince an undeniable profile of an individual, the demand to disarm the detective increases. But, at the very least, it can be argued, the type of "privacy invasion" accomplished by information-storing computers is of a different dimension than that caused by the use of surveillance devices that without consent intrude upon one's solitude or intimate relations.

Moreover, the alteration of traditional notions of privacy may be part of a psychologically healthy movement to "tell it like it is." Hypocritical social values are often spawned and perpetuated behind a curtain of privacy. The shame implied by the need to conceal true facts and feelings may reflect a denial of the intrinsic worth of man's individuality. While it has been suggested that privacy is an aspect of human dignity,[16] a more accurate perspective may reveal it as little more than an escape hatch from the vengeance of an intolerant society that accords no respect to the individual for what he *is*. If society were truly to acknowledge and nurture human dignity, the concept of privacy might become superfluous.[17]

The response to these arguments that minimize the significance of computers to the maintenance of privacy values is based more on value judgments than on logic. To ignore such judgments simply because they do not represent immutable truths misses the whole point of the privacy concept. While it is true that man can be conditioned out of the urge for privacy as it relates to specific situations, it is not likely that he can be led to forgo all manner of private life. As Alan Westin has indicated, privacy is closely related to the concept of personal autonomy that is an instinctive urge of all men.[18] The suggestion that man should be allowed to adapt to a changing world in which privacy is discarded is really quite sophistic.

---

16. *See* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964).

17. A homosexual under present values may live in constant peril of exposure. To him privacy is crucial to conceal or disguise every hint of his social aberration. However, if the homosexual were to be accepted for his intrinsic worth as a person with no regard to his personal sexual appetites, he could live freely and unself-consciously without the need for the constantly closed door.

18. The relevant remark did not escape Professor Miller's optical scanner. A. WESTIN, PRIVACY AND FREEDOM 34 (1967), is quoted as follows:

> [D]evelopment of individuality is particularly important in democratic societies, since quality of independent thought, diversity of views, and nonconformity are considered desirable traits for individuals. Such independence requires time for sheltered experimentation and testing of ideas, for preparation and practice in thought and conduct, without fear of ridicule or penalty, and for the opportunity to alter opinions before making them public. The individual's sense that it is he who decides when to 'go public' is a crucial aspect of his feeling of autonomy. Without such time for incubation and growth, through privacy, many ideas and positions would be launched into the world with dangerous prematurity. [p. 49.]

Man can also adapt to the industrial rape of the environment and in a generation view a polluted stream without a "pang of discomfort." The question raised by *The Assault on Privacy* is, Should he adapt or fight? It is certainly a valid question and one that must be answered before the decision becomes irrelevant.

With regard to the argument that semi-public information should not fall within the ambit of privacy protection, one must return to the personal autonomy aspects of human psychology. While thousands of people and organizations may know separate facts about an individual, so long as there is no centralization of these facts no one person or organization has the power to use the total information package to the individual's disadvantage. As Professor Miller puts it:

> [W]hen an individual is deprived of control over the spigot that governs the flow of information pertaining to him, in some measure he becomes subservient to those people and institutions that are able to manipulate it. [P. 25.]

Although freedom from the manipulation of semi-public information may be a facet of privacy distinct from those that relate to an individual's intimate relations and moments of self-searching solitude, it is cut from the same stone and merits careful concern.

The "tell it like it is" argument is a bit more facile. There can be no question that privacy is, among other things, a defense against the intolerances of society, and that the more intolerant the society the greater is the need for the shelter of secrecy. However, history has yet to produce the civilization without its biases and prejudices. In fact, the right to form negative opinions of those who diverge from deeply held moral values may be as important to a free society as the right of privacy itself. In the last analysis the issue should be one of personal choice, not public commandment. If an individual homosexual, for instance, chooses to run the gantlet of social disapproval and confront the injustice directly by making his life public, he should certainly be free to do so. It is not clear, however, that his more timid and psychologically frail counterparts ought to be drafted into the battle by a public policy that deprives them of their shields of privacy. If the key to privacy is individuality, the decision to dispense with privacy ought to be left in the hands of the individual.

III. Accuracy of Information

Another major danger of widespread computer surveillance pointed out in *The Assault on Privacy* really has nothing to do with privacy per se. This danger relates to the unjustified harm that can be done to a person who has inaccurate or misleading information in

his file. Once the right to acquire and use personal information is acknowledged, the way in which the data are collected and recorded becomes vital.

Professor Miller points out, with calculated effect, that a common source of credit information gathering is neighborhood gossip. This secondhand, often malicious information is translated into cold, hard-looking data in a computer printout, a process which illustrates what Miller refers to as the GIGO principle (Garbage In, Gospel Out). Furthermore, accurate but incomplete information also subjects the individual to contextual inaccuracies that distort the truth. Both of these dangers may be effectively mitigated by imposing tort liability upon those who cause harm through the use of inaccurate or misleading information, and by requiring that each data-subect be given notice of information contained in his file and an opportunity to set the record straight.

IV. Conclusion

The Assault on Privacy is a successful book. While it makes no attempt to cope with all the philosophical problems of privacy, it defines precisely the actual and threatened impact of computer technology on common concepts of privacy. By providing an explicit description of the present state of the problem and innumerable examples of what could happen, Professor Miller informs his reader of the considerations and consequences of modern technological developments. While *The Assault on Privacy* reveals the author's own biases, it supplies enough information to allow independent rational judgment. No more can be expected of a work of this kind.

Michael S. Josephson
Associate Professor of Law,
Wayne State University